

IN THE CLAIMS:

Amendments to the Claims are reflected in the listing of claims which begins on page 8 of this paper.

IN THE CLAIMS

1. (Currently Amended) A method of blocking unwanted e-mails, said method comprising the steps of:

determining that identifying an e-mail is unwanted;

determining a source IP address of said the unwanted e-mail; and

determining a registrant of said source IP address of said unwanted e-mail and querying an entity that manages registration of IP addresses to determining other source IP addresses ~~owned or registered by to said an owner or~~ registrant of the source IP address of said unwanted e-mail; and in response, subsequently blocking subsequent e-mails from ~~said source IP address~~ and said other IP addresses.

2. (Currently Amended) A method as set forth in claim 1 further comprising the step of blocking subsequent e-mails from said source IP address of said unwanted e-mail, wherein the ~~step of determining other source IP addresses owned or registered by an owner or registrant of the source IP address of said unwanted e-mail comprises the step of determining an owner or registrant of said source IP address of said unwanted e-mail.~~

3. (Currently Amended) A method as set forth in claim 2 wherein the step of determining ~~other source IP addresses owned or registered by an owner or~~ said registrant of the source IP address of said unwanted e-mail is performed by querying said an entity that manages registration of IP addresses.

4. (Currently Amended) A method as set forth in claim 13 wherein said entity is Internet Assigned Number Authority.

5. (Currently Amended) A method as set forth in claim 1 wherein the step of determining that identifying an e-mail ~~is~~ unwanted comprises the step of identifying an e-mail which is attempted to be sent to multiple recipients and where the e-mail contains the same or substantially the same text.

6. (Currently Amended) A method as set forth in claim 1 wherein the step of determining that identifying an e-mail ~~is~~ unwanted comprises the step of identifying an e-mail which is attempted to be sent to multiple recipients and where the e-mail contains the same or substantially the same subject line.

7. (Currently Amended) A method as set forth in claim 1 wherein the step of determining a source IP address of the unwanted e-mail comprises the step of reading the source IP address from a header of the unwanted e-mail.

8. (Currently Amended) A method as set forth in claim 2+ wherein the steps of subsequently blocking e-mails from said source IP address and blocking subsequent e-mails from said other IP addresses comprises the step of identifying said e-mails from said source IP address and said other IP addresses at a firewall or router, and ~~then~~ preventing them from passing through to a mail server(s) for their intended recipients.

9. (Currently Amended) A computer program product for blocking unwanted e-mails, said computer program product comprising:

a computer readable storage medium;

first program instructions to ~~determine~~identify ~~that~~ an e-mail ~~is~~is unwanted;

second program instructions to determine a source IP address of ~~said~~the unwanted e-mail;
and

third program instructions to determine a registrant of said source IP address of said unwanted e-mail and query an entity that manages registration of IP addresses to determine other source IP addresses owned or registered to said by an owner or registrant of the source IP address of said unwanted e-mail; and in response, fourth program instructions to subsequently block subsequent e-mails from said source IP address and said other IP addresses; and wherein

said first, second and, third ~~and fourth~~ program instructions are recorded on said computer readable storage medium.

10. (Currently Amended) A computer program product as set forth in claim 9 wherein said third program instructions also block subsequent e-mails from said source IP address of said unwanted e-mail, determine an owner or registrant of said source IP address of said unwanted e-mail;

11. (Currently Amended) A computer program product as set forth in claim ~~9~~10 wherein said third program instructions ~~determine an owner or~~ said registrant of said source IP address by querying ~~said~~an entity that manages registration of IP addresses.

12. (Currently Amended) A computer program product as set forth in claim ~~9~~¹¹ wherein said entity is Internet Assigned Number Authority.

13. (Currently Amended) A computer program product as set forth in claim 9 wherein said first program instructions determine that said~~identifies an~~ e-mail ~~is~~^{is} unwanted by identifying an e-mail which is attempted to be sent to multiple recipients and~~where the e-mail~~ contains the same or substantially the same text.

14. (Currently Amended) A computer program product as set forth in claim 9 wherein said first program instructions determine that said~~identifies an~~ e-mail ~~is~~^{is} unwanted by identifying an e-mail which is attempted to be sent to multiple recipients and~~where the e-mail~~ contains the same or substantially the same subject line.

15. (Currently Amended) A computer program product as set forth in claim 9 wherein said second program instructions ~~determines~~ a source IP address of said~~the~~ unwanted e-mail comprises by reading the source IP address from a header of said~~the~~ unwanted e-mail.

16. (Currently Amended) A computer program product as set forth in claim 9 wherein said fourth program instructions ~~blocks~~ subsequent e-mails from said source IP address and said other IP addresses by identifying said subsequent e-mails from said source IP address and said other IP addresses at a firewall or router, and ~~then~~ preventing them from passing through to a mail server(s) for their intended recipients.

17. (Canceled)

18. (Canceled)

19. (Canceled)

20. (Canceled)

Please enter new claims 21-28 as follows:

21. (New) A computer system for blocking unwanted e-mails, said computer system comprising:

first program instructions to determine that an e-mail is unwanted;

second program instructions to determine a source IP address of said unwanted e-mail;

third program instructions to determine a registrant of said source IP address of said unwanted e-mail and query an entity that manages registration of IP addresses to determine other source IP addresses registered to said registrant of the source IP address of said unwanted e-mail, and in response, block subsequent e-mails from said other IP addresses;

a computer readable storage media which stores said first, second and third program instructions; and

a CPU to execute said first, second and third program instructions.

22. (New) A computer system as set forth in claim 21 wherein said third program instructions also block subsequent e-mails from said source IP address of said unwanted e-mail.

23. (New) A computer system as set forth in claim 21 wherein said third program instructions determine said registrant of said source IP address by querying said entity that manages registration of IP addresses.

24. (New) A computer system as set forth in claim 21 wherein said entity is Internet Assigned Number Authority.

25. (New) A computer system as set forth in claim 21 wherein said first program instructions determine that said e-mail is unwanted by identifying an e-mail which is attempted to be sent to multiple recipients and contains the same or substantially the same text.

26. (New) A computer system as set forth in claim 21 wherein said first program instructions determine that said e-mail is unwanted by identifying an e-mail which is attempted to be sent to multiple recipients and contains the same or substantially the same subject line.

27. (New) A computer system as set forth in claim 21 wherein said second program instructions determine a source IP address of said unwanted e-mail by reading the source IP address from a header of said unwanted e-mail.

28. (New) A computer system as set forth in claim 21 wherein said fourth program instructions block subsequent e-mails from said source IP address and said other IP addresses by identifying said subsequent e-mails from said source IP address and said other IP addresses at a firewall or router, and preventing them from passing through to a mail server(s) for their intended recipients.